UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
2363 Bluelark Drive, Cincinnati, OH 45231

Case No. **1:23-MJ-00185**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1343	Wire fraud

The application is based on these facts:

See affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Benjamin Schild
Applicant's signature

Benjamin Schild, U.S. Postal Inspector
Printed name and title

Sworn to before me and signed in my presence, by reliable electronic means, specifically, FaceTime video conference.

Date: **Mar 13, 2023**

Stephanie K. Bowman
Judge's signature

City and state: Cincinnati, Ohio

Hon. Stephanie K. Bowman, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is **2363 Bluelark Drive, Cincinnati, OH** further described as a 3 bedroom, 1 bathroom red/brown brick exterior single-family home with dark window shutters.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 1343 (wire fraud), those violations involving Erlisa King and occurring after May 13, 2022, including:

a. Records and information relating to a scheme to defraud LeasingDesk[2];

b. Records and information relating to access of www.erenterplan.com;

c. Records and information relating to GreenDot Bank;

d. Records and information relating to any other bank accounts that received refunds from LeasingDesk;

e. Records and information relating to Ben's Automotive**.**

2. Computers or storage media used as a means to commit the violations described above, including a scheme to defraud LeasingDesk in violation of 18 U.S.C. § 1343.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

---

[2] As used herein, "LeasingDesk" refers to LeasingDesk Insurance Service and any of its parent companies, subsidiaries, or affiliated businesses, including but not limited to RealPage.

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF: **2363 Bluelark Drive, Cincinnati, OH 45231**	Case No. **1:23-MJ-00185**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Benjamin Schild, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **2363 Bluelark Drive, Cincinnati, OH 45231,** (hereinafter "PREMISES,") further described in Attachment A, for the things described in Attachment B.

2. I am an Inspector with the United States Postal Inspection Service (hereafter "USPIS") and have been since December 2019. I am currently assigned to the Mail Fraud team in the Cincinnati Field Office. In this capacity, I investigate criminal matters that are connected to the mail, including money laundering and various types of fraud. Prior to my employment with the USPIS, I served as a Special Agent in the United States Secret Service for 12 years. I have received training and investigative experience in interviewing, arrest procedures, search and seizure, search warrant applications, electronic media, and computer investigations, as it relates to white collar crime.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. In or about October 2022, LeasingDesk[1], a company that sells renter's insurance through its website (www.erenterplan.com), contacted the U.S. Postal Inspection Service to report that the company was the victim of a fraud scheme. Essentially, LeasingDesk reported that beginning on or about May 13, 2022, a person using the name Erlisa KING was using the website to buy hundreds of renter's insurance policies for apartments in the Cincinnati area, and then immediately cancelling the policies. When the policies were cancelled, LeasingDesk would immediately refund the initial premium, which was usually around $850, even if LeasingDesk had not actually collected the initial premium in the first place. Specifically, LeasingDesk reported that KING would sign up for a policy and supply a bank account routing number and account number to pay the initial premium. These routing numbers were legitimate, but the account numbers were bogus. A short time later, King would cancel the policy and request that the refund be sent to a debit card that she controlled (not the bogus bank account that she had

[1] As used herein, "LeasingDesk" refers to LeasingDesk Insurance Service and any of its parent companies, subsidiaries, or affiliated businesses, including but not limited to RealPage.

supplied when she ordered the policy). In this manner, King stole over $200,000 from LeasingDesk.

5. The evidence demonstrates that the perpetrator was Erlisa KING. To begin with, LeasingDesk provided a color copy of KING'S Ohio driver's license, which LeasingDesk had on file from some previous transactions with KING that pre-dated the fraud at issue here. Regarding the fraudulent transactions, LeasingDesk provided a spreadsheet of hundreds of transactions. The customer's name associated with these transactions was Erlisa KING. KING provided a variety of different Gmail addresses to LeasingDesk when she fraudulently applied for the policies. According to Google, the user-supplied name for many of these email addresses was Erlisa KING or some variation, such as Lisa KING. KING fraudulently applied for rental insurance policies for numerous apartments in the Apex apartment complex on Eastknoll Court in Cincinnati. King may have lived in this apartment complex in the past; according to records from Greendot Bank, KING opened a bank card using an address on Eastknoll Court in 2014.

6. According to LeasingDesk, KING directed most of the refunds to be sent to GreenDot Bank card number xxxx-xxxx-xxxx-0320. According to GreenDot Bank, this account is owned by Erlisa KING. The date of birth associated with the account is King's actual date of birth, though the Social Security number associated with the account does not match King's Social Security number on her OHLEG (Ohio Law Enforcement Gateway / Ohio driver's license) records. She also directed some of the refunds to be sent to Greendot card number xxxx-

xxxx-xxxx-9135. According to GreenDot, this account is also owned by Erlisa KING. The date of birth associated with this account is KING'S actual date of birth, and the Social Security number associated with the account matches KING'S Social Security number on her OHLEG records. GreenDot records for both cards reflect addresses for KING in Cincinnati.

7. Once the insurance refunds were deposited onto the GreenDot cards, the money was then withdrawn or spent. For example, KING spent $5,175 from the card ending in x0320 at Ben's Automotive in Cincinnati on May 25, 2022 as down payment on a 2014 Hyundai Equus luxury sedan (total price $22,932). The dealership kept photocopies of KING'S Ohio driver's license and the debit card ending in x0320. She made additional payments on the car on subsequent dates using the same GreenDot card.

8. Furthermore, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; or property designed for use, intended for use, or used in committing a crime may be found at the PREMISES. Over the course of several months, I have confirmed KING receives mail to the PREMISES address. In addition, on March 8, 2023, I observed KING arriving to the PREMISES in a newly purchased vehicle she obtained from Ben's Automotive, 6080 Colerain Ave, Cincinnati, OH 45239. The vehicle is a Black 2017 Infiniti QX80 and has been observed backed into the driveway of the PREMISES on several occasions.

9. I know from my training and experience that people often keep financial records, bank statements, mail, checks, and debit cards in their homes, sometimes for years. I also know from my training and experience that people often keep electronic storage devices, computers, and phones in their residences. I know from reviewing this case that a computer or electronic device connected to the internet was used by KING in the commission of these offenses. Specifically, the fraudulent insurance applications and refund requests were made through the internet.

TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

11. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

12. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer

users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

13. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the

attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used.

For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating

criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence

of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to commit online frauds, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

14. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded

on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

15. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

16. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

17. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

18. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. These documents discuss an ongoing criminal investigation that is not public. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Benjamin Schild

Benjamin Schild
Special Agent
U.S. Postal Inspection Service

Subscribed and sworn to before me on March 13, 2023, by reliable electronic means, specifically, FaceTime video conference.

Stephanie K. Bowman

STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE